Information-Age Warfare: A Working Bibliography, PartII

by Timothy L. Sanz

CYBERWAR, INFOWAR, information-based warfare, cyberterrorism, netwar, cyberpunks, information (or digital) warriors, information dominance, cyberspace defense, information chaos—these are just a few recent coinages reflecting the language dealing with the very broad topic of information-age warfare (I-AW). Publications on this subject are growing exponentially, and because of this and the growing importance of the topic, a pressing need exists to identify and classify the vast amount of literature that has been published on the topic in just the past three or four years. This bibliography strives to capture as much of the published, open-source literature as possible and contains citations to publications that have appeared generally since the beginning of 1992, to include citations to books, journals, newspapers and documents.[1] Due to the large volume of information warfare (IW) publications, this bibliography was published in two parts. The first part, published in the March-April 1998 issue, consisted of: I. Comparative Studies of Information-Based Conflict; II. Organizational Aspects of Information Conflict (nonstate actors and networks); III. Perception Management, Psychological Operations (PSYOP) and Deception Issues; and IV. Revolution in Military Affairs (RMA).

The research sources of a multitude of databases, CD-ROMs and indexes were used, including those of the Naval Postgraduate Library, Stanford University, University of California at Berkeley, the Monterey Institute of International Studies, National Defense University (NDU) Library, Pentagon library and the Combined Arms Research Library at Fort Leavenworth, Kansas.[2] The bibliography is arranged alphabetically under each subject category by author, or title if no author is indicated. It is categorized into the following broad subject categories, with a brief explanation of each category's scope:

V. Cyberspace and Security Issues. Includes publications concerning issues of hackers, sabotage, disruption or destruction of computer-telecommunication systems and/or data.

VI. Electronic-Technical Dimensions (including command, control, communication, computers and intelligence [C^{4}I] issues). Includes articles dealing strictly with technical aspects of computer systems such as data storage and retrieval issues, digitization, information chaos issues and offensive-defensive capabilities.

VII. Internet Sites. Includes only a few of the main sites from which to launch searches to other sites.

The term infomation-age warfare appeared in this article 43 times. For brevity, we use the acronym I-AW. Readers should understand that I-AW is not an approved acronym. The term and elsewhere *appeared in this article 42 times. For brevity, we use the symbol +. Readers should understand that these changes apply only to this bibliography.—Editor*

V. Cyberspace and Security Issues

Acherman, Robert K. "Digital Formats Complicate Information Security Tasks." *Signal*, February 1997, 21-23. Focuses on how US planners are now paying considerable attention to the defensive aspect of I-AW and the degrading or destroying of data.

Adams, Charlotte. "Information Warfare Takes a Front Seat." *Military & Aerospace Electronics*, June 1996, 19-21. Addresses operational security application within the Defense Management System, evolution of the Defense Advanced Research Projects Agency Information Survivability program and the National Security Telecommunications Advisory Council's focus on information protection and assurance.

Aldrich, Richard W. "The International Legal Implications of Information Warfare." *Airpower Journal*, Fall 1996, 99-110. Reviews definition of IW and debates the appropriateness of applying the law of war to IW techniques.

Allard, Kenneth. "Data Transforms Warfare." *Defense News*, 4 March 1996, 24. Discusses how I-AW poses new challenges to corporate culture.

Anthes, Gary H. "DOD on Red Alert to Fend off Info Attacks." *Computerworld*, 6 January 1997, 1-2. Department of Defense (DOD) to establish a Red team of computer security experts to assess the security of computer and communications systems and determine the extent and nature of threats to the US information infrastructure.

_____. "Feds Limit Info Warfare Role." *Computerworld*, 18 September 1995, 24. Reports on statements by senior law enforcement and intelligence agencies at the 1995 Third International Information Warfare Conference that they would not take part in industrial espionage against foreign firms or countries even though US companies are asking for help.

_____. "Info-Terrorist Threat Growing." *Computerworld*, 30 January 1995, 1-2. Contends that few information system managers pay attention to the dangers of electromagnetic weapons and that corporate preparation to address this threat is currently scant.

_____. "Info Warfare Risk Growing." *Computerworld*, 22 May 1995, 1, 16. Reports on US military officials' assessments concerning the threat and describes some DOD weapons such as electromagnetic pulse guns and sleeper computer viruses; describes the establishment of I-AW centers by all three

branches of the Armed Forces to study threats to US information.

_____. "New Laws Sought for Info Warfare." *Computerworld*, 5 June 1995, 55. Addresses the need for new laws to govern I-AW in the US and a legal framework to protect information systems.

_____. "Security Pundits Weigh War Threat." *Computerworld*, 2 October 1995, 71. Reviews the opinions of experts at a conference on I-AW that networks of US companies are vulnerable.

_____. "U.S. Easy Target for Cyberattacks." *Computerworld*, 27 May 1996, 7. Reports on the lack of security in the US government's computer network and the computer industry's slow response.

Arnold, H.D. et al. "Targeting Financial Systems as Centers of Gravity: 'Low Intensity to No Intensity' Conflict." *Defense Analysis*, 10/2 (1994), 181-208.

"Axent Announces Contract Win to Protect AF Bases from Information Warfare." *C4i News*, 6 November 1997, 1.

Benedikt, Michael, ed. Cyberspace: First Steps. Cambridge, MA: M.I.T., 1991. Provides a compilation of papers presented at The First Conference on Cyberspace in 1990; characterizes cyberspace as "an infinite artificial world where humans navigate in information-based space" and as "the ultimate computer-human interface."

Black, Steven K. *A Sobering Look at the Contours of Cyberspace*. Ridgway Viewpoints no. 96-3. Pittsburgh, PA: Ridgway Center for International Security Studies, University of Pittsburgh, 1996. Covers security aspects of computer networks and telecommunications.

Bond, J.N. *Peacetime Foreign Data Manipulation as One Aspect of Offensive Information Warfare: Questions of Legality under the United Nations Charter Article 2(4)*. Newport, RI: Naval War College (NWC), 14 June 1996. Discusses the issue of whether manipulation of a foreign state's data may be considered use of force against that country in violation of Article 2(4) of the UN Charter; examines briefly whether Article 2(4) is still a valid norm under international law; concludes that in certain circumstances data manipulation could be considered the use of force but is more likely to be viewed as an intervention in the internal affairs of the foreign state.

"Businesses Face Threat of Information Warfare." *Signal*, June 1996, 45-46.

Campen, Alan D. et al., ed. "Cooperative Effort Encourages Safe Information Highway Travel." *Signal*, October 1995, 43-44.

_____. *Cyberwar: Security, Strategy, and Conflict in the Information Age*. Fairfax, VA: AFCEA International Press, 1996.

_____. "Rush to Information-Based Warfare Gambles with National Security." *Signal*, July 1995, 67-69.

_____. "Vulnerability of Info Systems Demands Immediate Action." *National Defense*, November 1995, 26-27.

Carr, Thomas H. *War on the Cheap. Using Information Warfare to Lengthen the Decision Cycle*. Newport, RI: NWC, 12 February 1996. Investigates how a US adversary might indirectly attack a military operation's center of gravity (COG) by disrupting operational tempo using I-AW; shows how a financially limited country could effectively fight the US military by paying talented computer hackers and others familiar with US support networks to disturb these systems; concludes that a good I-AW capability would be a great combat multiplier for any foe and is not a capability realized sufficiently by US military joint planners.

Cheswick, William and Steven Bellovin. *Firewalls and Internet Security: Repelling the Wily Hacker*. Boston: Addison-Wesley, 1994.

"CIA Director Warns Information Warfare Poses Danger to U.S." *Wall Street Journal*, 26 June 1996, B6(E). Reports on Director John Deutch's warnings about the vulnerability of internet communications to computer-based cyber attacks.

Clapper, James R. Jr. and Eben H. Trevino Jr. "Critical Security Dominates Information Warfare Moves." *Signal*, March 1995, 71-72.

"Commanders Pull Intelligence in Information Warfare Strategy." *Signal*, August 1994, 29-31.

"Commercial, Military Information Security Requirements Meld." *Signal*, May 1996, 108-9.

Cooper, Pat. "Cyberwar Recasts National Security." *Army Times*, 26 June 1995, 26. Describes the emergence of I-AW as the chief means of deterring adversaries and defending US interests, the deterrent value of being able to cripple another society by destroying its information systems and the protection of computer networks, systems and data.

_____. "Internet Link to Defense Data May be too Easy." *Army Times*, 22 January 1996, 27+. Reviews cases of hackers gaining access to and leaking secret military information; includes comments from computer security consultant James Lightburn.

_____. "New Effort Afoot to Keep Ships' Computers Afloat." *Navy Times*, 20 November 1995, 31. Outlines US Navy plans to invest $389 million in 1995 to protect ships from attacks on their computer networks.

_____. "Newest Information Warfare Technology Could Backfire On Battlefield of the Future." *Defense News*, 6 May 1996, 26.

_____. "War Game Reveals IW Vulnerabilities." *Defense News*, 4 March 1996, 33.

Croal, N'Gai and Jennifer Tanaka. "Gunning for Bytes." *Newsweek*, 10 June 1996, 11. Reports on the US Air Force's designation of a 20-person squadron in South Carolina as an information-warfare unit which will study both offensive and defensive strategies.

"Crucial Network Imperatives Spawn Information War Peril." *Signal*, June 1996, 35-38.

"Cyberterrorism Threatens Online Security; Federal Panel Cites 'Weapons of Mass Disruption'." *Computerworld* 31/41 (1997), 14.

Dellecave, Tom Jr. "Insecurity: Is Technology Putting Your Company's Primary Asset—its Information—at Risk? *Sales & Marketing Management*, April 1996, 38-50. Discusses the firm InfoWar Inc., which discovers vulnerabilities in companies' computer security.

Deming, Peter. *Computers Under Attack: Intruders, Worms and Viruses*. ACM Press.

DOD. *Defensive Information Warfare Implementation*. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01A, 31 May 1996. Contains sections on elements of the IW-defense process, information system protection, responsibilities of commanders and agencies and other topics; includes a list of references in Enclosure E to many governmental directives on electronic security.

Esarey, Clinton D. *Media and the U.S. Army: You Don't Always Get What You Want; You May Just Get What You Need*. Fort Leavenworth, KS: School of Advanced Military Studies (SAMS), US Army Command and General Staff College (CGSC), 23 May 1994. Discusses the information operations (IO) concept that the US Army is developing which describes the framework for conducting I-AW; examines the characteristics of the US media—Army relationship in the 21st century.

Evancoe, Paul R. and Mark Bentley. "Computer Viruses Loom As Future Era Weapons." *National Defense*, February 1994, 19, 21. Describes the types and uses of computer viruses for disrupting military weapons and information systems, especially fire control, targeting, intelligence and banking.

Evers, Stacey. "Stopping the Hacking of Cyber Information." *Jane's Defence Weekly*, 10 April 1996, 22-25.

Farrell, Peter T. *A National Security Strategy for Information Assurance*. Carlisle Barracks, PA: AWC, 1997.

Fialka, John J. "Pentagon Studies Art of 'Information War-

fare' to Reduce its Systems' Vulnerability to Hackers." *Wall Street Journal*, 3 July 1995, A20. Discusses a report by The Defense Information Systems Agency (DISA) that hacker attacks on the Pentagon's global computer networks average about two a day; describes help received from the National Security Agency (NSA).

"FIWC Commissioned." *Naval Aviation News*, January-February 1996, 2. Describes the mission of the US Navy's newly commissioned Fleet Information Warfare Center (FIWC) Naval Amphibious Base, Little Creek, Virginia.

Gambel, Daniel W. "MLS (Multi-Level Security): Data Security for the DOD and the Rest of Us." *Defense Electronics*, June 1995, 10+.

Greenberg, Lawrence T. *Old Law for a New World?: The Applicability of International Law to Information Warfare*. Stanford, CA: Center for International Security and Arms Control, Institute for International Studies, Stanford University, 1997.

Griffith, Thomas E. *Strategic Attack of National Electrical Systems*. Maxwell Air Force Base (AFB), AL: Air University, 1994. Contends that strategic attacks on national electrical systems have generally failed to meet their objectives because of a failure to understand how nations use these systems; argues that the US should reject future attacks on national electric power systems.

Guilbault, R.G. "Information Empowerment: The Key Force Multiplier." *Defense & Security Electronics*, January 1996, 10+.

"Hackers, Beware on Defense." *Navy Times*, 14 August 1995, 30. Reports on the Anti-Electronic Racketeering Act proposed in the Senate, protection of military information systems and the difficulty of prosecuting hackers.

Hardy, Stephen M. "New Guerrilla Warfare." *Journal of Electronic Defense*, September 1996, 46+. Addresses protecting DOD computer and communications assets.

_____. "A Question of Symmetry?" *Journal of Electronic Defense*, January 1997, 42-44+. Describes common uses of cryptography and some encryption alternatives available to armed forces worldwide.

Hughes, David. "609th Sqdn. Pursues New Realm of Combat." *Aviation Week & Space Technology*, 29 April 1996, 52-53. Describes the US Air Force's 609th IW Squadron, formed to protect vital computer networks in a central command air operations center and the challenges facing it in protecting these networks.

Hundley, Richard et al., rapporteurs. *Security in Cyberspace: Emerging Challenges for Society: Proceedings of an International Conference*. Santa Monica, CA: RAND Corporation, 1996.

Hundley, Richard and Robert H. Anderson. *A Qualitative Methodology for the Assessment of Cyberspace-Related Risks*. Santa Monica, CA: RAND Corporation, 1996.

Hurst, Gerald A. *Taking Down Telecommunications*. Maxwell AFB, AL: Air University, 1994. A 76-page report examining the vulnerabilities of national systems to lethal and nonlethal attacks; calls for a strong research and development (R&D) program to acquire nonlethal technologies with which to attack and disable enemy communications.

Information Security: Computer Attacks at Department of Defense Pose Increasing Risk. Washington, DC: Government Accounting Office (GAO), GAO/AIMD-96-84, May 1996.

"Information Systems, Networks Spark Major Security Challenges." *Signal*, June 1996, 43.

Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance. 2d ed. Science Applications International Corporation, 4 July 1996. A study commissioned by the Joint Staff to identify and document organizational and other conditions as an educational baseline in the formulation of a comprehensive information protection strategy; contains chapters on infrastructures, the legal, regulatory, policy, technology and intelligence environment and organizational considerations.

"Information Warriors Raze Enemy's Vital Data Chains." *National Defense*, March 1995, 30-31.

"Infowar Convention Raises Security Issues." *Computer Fraud and Security* 11 (1996), 6.

Kabay, M.E. "Prepare Yourself for Information Warfare." *Computerworld*, 20 March 1995, ss2-7. Deals with threats to companies' information infrastructure, industrial espionage, risk management, security systems and other technology issues.

Kaneshige, Thomas. "Is the US Prepared for Cyberwar?" *Computer*, 1 July 1996, 20-1. Discusses the threat posed by strategic I-AW which could cripple an enemy's electronic commerce, power grid and air traffic control and phone systems.

Kennedy, K.J., B.M. Lawlor and A.J. Nelson. *Grand Strategy for Information Age National Security*. Carlisle Barracks, PA: AWC, 12 May 1996. Examines current national security strategy which the authors contend is obsolete, fails to defend against structured information attacks threatening US COGs and relies upon DOD as sole provider of national defense in the information dimension; sets forth a strategic plan for information assurance.

Klinefelter, Stephen. *The National Security Strategy and Information Warfare*. Carlisle Barracks, PA: AWC, 1997.

Kovacich, Gerald. "Information Warfare and the Information System Security Professional." *Computers & Security* 16/1 (1997), 14+.

Kuschner, Karl W. *Legal and Practical Constraints on Information Warfare*. Newport, RI: NWC, 14 June 96. Discusses tests for necessity and proportionality under the laws of armed conflict, the need for weighing the possible consequences of this type of warfare and problems such as lack of enemy command and control (C^2), posthostility reconstruction and retaliation.

Landay, Jonathan S. "US Worries about Growing Threat of 'Cyberwar' in Information Age." *Christian Science Monitor*, 7 June 1996, 1. Describes the mounting apprehension about the threat of cyberwar as the nation's military, financial, government and business sectors become more interlinked and dependent on proliferating communication networks worldwide.

Lange, Larry. "Warnings for an Electronic Nation." *Electronic Engineering Times*, 22 September 1997, 93+.

Lawlor, Maryann. "Science Board Task Force Challenges Defensive Information Warfare Status." *Signal*, September 1997, 63+.

"Lawmakers Get Education on Perils of Cyber Warfare." *C4i News*, 27 March 1997.

Libicki, Martin C. *Defending Cyberspace and Other Metaphors*. Washington, DC: NDU, 1997.

_____. "Information Warfare: A Brief Guide to Defense Preparedness—Information Systems Play an Important Role in Society, So Threats to Their Security Should Be Taken Seriously—But There is No Need to Panic." *Physics Today* 50/9 (1997), 40.

Lohr, Steve. "National Security Experts Plan for Wars Whose Targets and Weapons Are All Digital." *New York Times*, 30 September 1996, D1. Discusses I-AW exercises conducted by the NDU and the DOD and the growing reliance on computer networks and telecommunications which makes the United States vulnerable to I-AW; includes comments of Howard Frank, Martin Libicki, John Deutch and William Marlow.

Machlis, Sharon. "Security Experts: Hacker Detection is Key." *Computerworld*, 3 March 1997, 59, 67. Reports on DISA's IW Division and discusses the need to concentrate on detecting intruders and shutting down access to computer systems.

Madsen, Wayne. "Information Warfare." *Information Systems Security*, Fall 1995, 12-15. Discusses potential capabilities of the US government, the Defense Science Board's (DSB's) "Information Architecture for the Battlefield" and the Computer Security Act of 1987.

_____. "Intelligence Agency Threats to Computer Security." *International Journal of Intelligence and Counterintelligence*, Winter 1993, 413-88. Contains a country-by-country listing of computer espionage capabilities of intelligence and law enforcement agencies.

Mann, Paul. "Cyber Threat Expands with Unchecked Speed." *Aviation Week & Space Technology*, 8 July 1996, 63-64. Reviews the potential of I-AW threatening the disruption of the US air traffic control system, banking networks and powerplants.

Matthews, William. "Susceptible to Sabotage." *Air Force Times*, 5 February 1996, 28. Reviews the threat to automated information systems.

Maze, Rick. "Military computers vulnerable to intrusion." *Navy Times*, 29 July 1996, 25+. Details the testimony of Deputy Defense Secretary John P. White before the US Senate Governmental Affairs Investigations Subcommittee on the vulnerability of US government computers to hackers and intruders; describes the military's information network and calls for increased security measures.

McCollum, William W. *The Role of the Intelligence Community in Preparing to Win the Information War*. Carlisle Barracks, PA: AWC, 1997.

McKenna, James T. "Rome Lab Targets Info Warfare Defenses." *Aviation Week & Space Technology*, 12 August 1996, 65-66. Discusses the work of researchers at the US Air Force's Rome Laboratory investigating software and technologies to better protect critical military and civil information systems and data.

_____. "Tighter Security Urged for Defense Computers." *Aviation Week & Space Technology*, 20 January 1997, 60-61.

McKenna, Pat. "Hacker Trackers: OSI (Office of Special Investigations) Computer Cops Fight Crime On-line." *Airman*, April 1996, 24-29. Discusses the work of the US Air Force IW Center.

Messmer, Ellen. "Report Pushes for Military Buildup on the Net." *Network World*, 20 January 1997, 31. Discusses a DOD report on the high potential for I-AW against civilian and government organizations and its request for $5 billion for enhanced defensive electronic warfare (EW) countermeasures.

Metzgar, Terry. "Hostile Intercepts Aimed At Information Systems." *National Defense*, May-June 1993, 24-26. Examines corporate espionage and the $10 billion-a-year information security market; covers specific threats, such as from eavesdropping, data interception and electromagnetic induction and countermeasures available.

Molander, Roger C. et al. "Strategic Information Warfare: A New Face of War." *Parameters*, Autumn 1996, 81-92.

_____. *Strategic Information Warfare: A New Face of War*. Santa Monica, CA: RAND Corporation, 1996. A 110-page report prepared for the Office of the Assistant Secretary of Defense—Command, Control, Communications and Intelligence (C^3I); provides perspectives on a broad range of potential national security issues; studies the ongoing rapid evolution of cyberspace—the global information infrastructure—and the growing dependence of the US military and other national institutions and infrastructures on potentially vulnerable elements of the national information infrastructure.

Munro, Neil. "The Pentagon's New Nightmare: An Electronic Pearl Harbor." *Washington Post*, 16 July 1995, C3.

_____. "Reno Proposes Cyberspace Defense." *Washington Technology*, 25 April 1996, 53-54.

_____."Sketching a National Information Warfare Defense Plan." *Communications of the ACM*, November 1996, 15-17. Describes the executive order "Critical Infrastructure Protection" which creates a defense policy for protecting the country's phone systems, power grid, air traffic control and bank systems, establishes a commission to formulate a national I-AW or cyberwar defense plan and forms an ad-hoc, multiagency network defense organization led by the Federal Bureau of Investigation to boost defenses in the near term.

_____. "White House Edges Closer to Cyberwar." *Washington Technology*, 21 March 1996, 12.

Mussington, David. "Systematic Intrusions in DOD Computer Systems." *Pointer* (Monthly supplement to *Jane's Intelligence Review*) August 1996, 16.

_____. "Throwing the Switch in Cyberspace." *Jane's Intelligence Review*, July 1996, 331-34. Assesses the emergence of global information networks and the potential use of these networks for terrorist or criminal purposes; discusses information-layer and infrastructure-layer issues, network vulnerabilities and other topics.

National Research Council. *Computers at Risk: Safe Computing in the Information Age*. Washington, DC: National Academy Press, 1991.

"No Sheriffs Patrol Universal Cyberspace Frontier Towns." *Signal*, June 1996, 39-42.

Orr, Joseph E. *Information Dominance: A Policy of Selective Engagement*. Carlisle Barracks, PA: AWC, 1997.

Peterson, A. Padgett. "Tactical Computers Vulnerable To Malicious Software Attacks." *Signal*, November 1993, 74-75. Examines the vulnerability of tactical computer systems used by the US military and some potential countermeasures; contends that the denial of information to an adversary by using computer viruses and logic bombs can be more valuable than the ability to intercept transmissions.

Planning Considerations for Defensive Information Warfare: Information Assurance. Arlington, VA: DISA, 1993. Calls for the protection of the defense information infrastructure upon which the US military depends; discusses 12 crucial considerations in planning defensive I-AW to maintain operational readiness and safeguard national security.

Platt, Charles. "Hackers: Threat or Menace?" *Wired*, November 1994, 82-85.

"Policy Forum: Pearl Harbor in Information Warfare?" *The Washington Quarterly* 20/2 (1997), 39+.

Power, Richard. "CSI Special Report On Information Warfare." *Computer Security Journal*, October 1995.

_____. *Current and Future Danger: A CSI Primer on Computer Crime and Information Warfare*. San Francisco, CA: Computer Security Institute, 1995.

"Rapid Technology Growth Spawns Land Information Warfare Activity." *Signal*, July 1996, 51-54. Reports on the Army Intelligence and Security Command.

"Redundancy, Robustness Protect Vital National Information Links." *Signal*, May 1996, 36-39.

Ricks, Thomas E. "Information-Warfare Defense is Urged: Pentagon Panel Warns of 'Electronic Pearl Harbor.'" *Wall Street Journal*, 6 January 1997, B6(W), B2(E). Reviews the DSB's task force recommendations which includes spending an additional $3 billion over the next five years to improve the security of the nation's telecommunications and computing infrastructure and securing legal authority to launch counterattacks against computer hackers.

Robinson, Clarence A. Jr. "Defense Organization Safeguards War Fighters' Information Flow." *Signal*, October 1995, 15-18. Reports on DISA.

_____. "Electronic Combat Techniques Provide Information War Edge." *Signal*, July 1995, 33-35.

_____. "Information Warfare Strings Trip Wire Warning Strategy." *Signal*, May 1996, 29-33.

Ronfeldt, David F. *Cyberocracy, Cyberspace, And Cyberology: Political Effects of the Information Revolution*. Santa Monica, CA: RAND Corporation, 1991. Examines how the information and communications technology revolution may ultimately affect business, politics and government; contends that information and its control will become a dominant source of power.

Ross, Mitchell S. *National Information Systems: The*

Archilles Heel of National Security. Carlisle Barracks, PA: AWC, 1997.

"Safeguarding the Info Highway." *Navy Times*, 16 October 1995, 26. Reports on US government agencies' response concerning the threat to interconnected banking and telecommunications networks and the selection of the Federal Emergency Management Agency to lead an interagency plan.

Sakkas, Peter E. "Espionage and Sabotage in the Computer World." *International Journal of Intelligence and Counterintelligence*, Summer 1991, 155-202. Discusses the issues, tactics and countermeasures of waging EW against military or corporate targets with simply a telephone, computer, modem and the appropriate software; reports on viruses, trojan horses, logic bombs, worms, trapdoors and the most sinister genetic-based viruses.

Schwartau, Winn. *Information Warfare: Chaos on the Electronic Superhighway*. New York: Thunder's Mouth Press, 1994. Addresses computer security and crime issues.

_____."Information Warfare: Chaos on the Electronic Superhighway." *Marine Corps Gazette*, October 1994, 79-80.

_____. *Information Warfare: Cyberterrorism: Protecting Your Personal Security in the Electronic Age*. 2d ed. New York: Thunder's Mouth Press; Emeryville, CA: Distributed by Publishers Group West, 1996.

Schwartz, John. "Retired General's Mission: Making Cyberspace Secure; Dangers of 'Information Warfare' Rising, Marsh Says." *Washington Post*, 31 January 1997, A19. Presents an interview with Robert T. Marsh, chairman of the President's Commission on Critical Infrastructure Protection.

Schwartzstein, Stuart J.D. ed. *The Information Revolution and National Security: Dimensions and Directions*. With a foreword by William A. Owens. Washington, DC: Center for Strategic and International Studies, 1996.

Shenon, Philip. "Defense Dept. Computers Face a Hacker Threat, Report Says: Growing Danger to U.S. Security is Cited." *New York Times*, 23 May 1996, A11(N), A22(L). Discusses a report from the GAO concerning Pentagon vulnerability to attack from hackers and the estimated 250,000 attacks made on its computer network in 1995.

Slatta, Michelle and Joshua Quittner. *Masters of Deception: The Gang that Ruled Cyberspace*. New York: HarperCollins, 1995. Examines the cybergang of teenagers who penetrated the New York telephone system and tapped into sensitive personal and financial databanks.

Sussman, Vic. "Is Anything Safe in Cyberspace?" *U.S. News and World Report*, 23 January 1995, 55-60.

Thomas, Timothy L. "Deterring Information Warfare: A New Strategic Challenge." *Parameters*, Winter 1996-1997, 81-91. Examines theoretical aspects of assaults on information-based assets and the lack of ways in dealing with this form of attack on national sovereignty.

Thomas, T.R. *InfoWar, InfoTheft and InfoSec*. Los Alamos, NM: Los Alamos National Laboratory; Washington, DC: Department of Energy, 1993. A summary of the 1993 Davis Computer Security Workshop sponsored by the NSA's Office of Information Security and the Air Force's Cryptologic Support Center; focuses on the seriousness and sophistication of the real and potential threats to the integrity of the country's information systems.

Thompson, Mark and Douglas Waller. "If War Comes Home." *Time*, 21 August 1995, 44-46. Reports on the wargame, "The Day After . . . in Cyberspace," conducted by the RAND Corporation, which simulated an I-AW attack on the US and its allies; describes the DISA which provides protection to the military's computers.

Thompson, Michael J. *Information Warfare—Who is Responsible?: Coordinating the Protection of Our National Information Infrastructure*. Carlisle Barracks, PA: AWC, 1997.

Wallich, Paul. "Wire Pirates." *Scientific American*, March 1994, 90-101. Examines the dark side of the information revolution associated with electronic criminals.

Weiner, Tim. "Head of C.I.A. Plans Center To Protect Federal Computers." *New York Times*, 26 June 1996, B7. Reports on the announcement by Central Intelligence Agency (CIA) Director John M. Deutch of the creation of a "cyberwar" center at NSA to protect against attacks on computers in DOD's war rooms, air traffic control and financial transfers.

Welch, Jonathan. "International Money Market: A Weapon in Waiting? *Royal United Services Institute (RUSI) Journal*, April 1996, 34-40.

Whisenhunt, Robert H. *Information Warfare and the Lack of a U.S. National Policy. Study Project*. Carlisle Barracks, PA: AWC, 15 April 1996. Discusses the profound impact of the information technology (IT) explosion on the US information infrastructure; suggests that the executive branch place responsibility on a single agency or committee to integrate fragmented efforts by many agencies and departments into a coherent program for national security.

VI. Electronic-Technological Dimensions (to include C^4I issues)

Acherman, Robert K. "Command, Control Simulation Develops Information Warriors." *Signal*, February 1997, 25-28. Describes the US Air Force's fifth Fort Franklin, battlespace field laboratory exercise and vulnerabilities in battlefield systems at Hanscom AFB, Massachusetts.

_____. "Military Planners Gird for Information Revolution." *Signal*, May 1995, 71-72+.

_____. "Navy Doctrine, Systems Face Information Warfare Makeover." *Signal*, July 1996, 57-60.

"Advanced Information Systems Impel Operational Technologies." *Signal*, March 1996, 41-43.

Alberts, David S. *Defensive Information Warfare*. Washington, DC: Directorate of Advanced Concepts, Technologies and Information Strategies, NDU, August 1996. An 82-page report assessing the problem of defending against I-AW; stresses the need to focus on two goals: protect against catastrophic events and continually raise the cost of mounting an attack and mitigate the expected damage.

_____. *The Unintended Consequences of Information Age Technologies*. Washington, DC: Center for Advanced Concepts and Technology, Institute for National Strategic Studies, NDU, 1996.

Alexander, David. "Information Warfare and the Digitized Battlefield." *Military Technology*, September 1995, 57-64.

"Army Plan Fosters Dynamic Information War Framework." *Signal*, November 1993, 55-58. Covers C^3 issues and information storage and retrieval systems.

Arnold, Wallace C. and Thomas H. Killion. "Soldier-information Interface." *Army RD&A Bulletin*, January-February 1995, 7-10. Discusses military equipment design, ergonomics and cognitive functions.

Arquilla, John. "Strategic Implications of Information Dominance." *Strategic Review*, Summer 1994, 24-30. Describes the possible emergence of a new paradigm—control warfare—that will supersede its attrition- and maneuver-oriented predecessors; discusses how over time the new strategies, doctrines and force postures will be imitated widely, leveling the field and allowing the reincorporation of older attritional and maneuver techniques.

Ashman, Bruce W. *Defensive Information Warfare in Today's Joint Operations: What's the Real Threat?* Carlisle Barracks, PA: AWC, 1997.

"Avoiding Information Overload Assists Commanders' Battlefield Performance." *Signal*, August 1995, 35+.

Belknap, M. *Military Decision Making in The Information Age*. Newport, RI: Joint Military Operations Department, NWC, 12 February 1996. Analyzes three critical aspects of military decision making that will be most affected by enhancements in IT—certainty, tempo and C^2, with tempo becoming the most critical aspect of future decision making.

Betzold, Victor A. "Data Storage and Retrieval for the Digital Battlefield." *Army RD&A Bulletin*, November-December 1995, 26-29. Focuses on military technology R&D.

Blanchette, Joel G. "USACAPOC's FOCUS Project: Waging the War for Information." *Special Warfare*, January 1996, 45-49. Reports on the US Army Civil Affairs and PSYOP Command project to link personnel information databases.

Blazar, Ernest. "Planners: Information is the Best Weapon." *Navy Times*, 5 September 1994, 8. Describes the creation of the Navy Information Warfare Activity on 18 August 1994 by the US Navy, its core members, headquarters and goals.

Blount, Kerry A. "Wrestling with Information Warfare's 'Dark Side.'" *ARMY*, February 1996, 9-12. Addresses the lack of systematic efforts to deal with command and control warfare (C^2W).

_____. "A Two-component Strategy for Winning the Information War." *ARMY*, January 1995, 10-11. Discusses the need to combine C^2W with C^4I.

Boorda, Jeremy M. "Copernicus Forward: C^4I for the 21st Century." *Surface Warfare*, July-August 1995, 2-7.

_____. "Leading the Revolution in C^4I." *Joint Force Quarterly (JFQ)*, Autumn 1995, 14-17

Braunberg, Andrew C. "Air Force Pursues Two-sided Information Warfare Strategy." *Signal*, July 1996, 63-65.

Busey, James B. IV. "Information Warfare Calculus Mandates Protective Actions." *Signal*, October 1994, 15+.

Calvo, Mark D. "Digitizing the Force XXI Battlefield." *Military Review*, May-June 1996, 68-70.

Campen, Alan D, ed. *The First Information War: The Story of Communications, Computers and Intelligence Systems in the Persian Gulf War*. Fairfax, VA: Armed Forces Communications and Electronics Association International Press, 1992. Contains 23 articles concerning the use of knowledge and information during the Persian Gulf War.

Canavan, Gregory H. *Simulation, Computing, Information and Future Warfare*. Los Alamos, NM: Los Alamos National Laboratory, 1993.

Caravella, Frank J. " ADA's Role in Winning the Information War." ADA: *Air Defense Artillery*, September-October 1995, 2-3.

Caruth, Greg and Collie J. Johnson. "Program Manager Interviews Anita Jones, Director, Defense Research and Engineering." *Program Manager*, July-August 1996, 2-8. Reports on DOD procurement and technological R&D issues dealing with I-AW.

"CIA Seeks Ties with Industry." *Aviation Week & Space Technology*, 8 July 1996, 64+. Discusses the CIA's forging of relationships with the aviation industry to address the cyberspace warfare threat to international commerce.

Clark, Wesley K. "Digitization: Key to Landpower Dominance." *ARMY*, November 1993, 28-33.

Cooper, Pat. "Pentagon Debates Potential of Information Warfare." *Defense News*, 13 May 1996, 3+.

Cunningham, W.B. and M.M. Taylor. "Information for Battle Command." *Military Review*, November 1994, 81-84.

Cyberwar! *Current Events*, 30 October 1995, 2a-2d. Assesses computer technology in the 21st century, its implications for IW and ways in which military strategy is changing to take advantage of new technology.

Czerwinski, Thomas J. "Command and Control at the Crossroads." *Marine Corps Gazette*, October 1995, 13-15.

Davison, David A. and Steve Taulbee. "Digitizing the Battlefield." *Army RD&A Bulletin*, May-June 1995, 49-51. Examines US Army IT and the Army Research Laboratory.

de Borchgrave, Arnaud. "Is America at Risk in a Cyberwar?" *Insight on the News*, 11 March 1996, 48. Discusses the alarming results of the Pentagon's EW scenario and America's vulnerability to EW.

Deitchman, S.J. "Information Warfare." *Issues in Science and Technology* 12/2 (1996), 15-17.

"Digitized Zephyr Lifting Fog from No Man's Land: Army Pushes Information Warfare Transition." *National Defense*, September 1995, 32-33.

Dishong, Donald J. *On Studying the Effect of Information Warfare on C^2 Decision Making*. Monterey, CA: Naval Postgraduate School, June 1994. Uses a software package called Tactical Tic-Tac-Toe (T^4) to simulate C^2 decisions made in an I-AW environment; shows that delaying one's immediate opponent from grasping the tactical picture greatly enhances the chances of increasing one's effectiveness and that delaying the enemy's understanding of "pieces" of the strategic picture also dramatically increases effectiveness.

DOD. *Joint Command and Control Warfare Policy*. Chairman of the CJCSI 3210.3, 1 August 1996.

DOD, Deputy Assistant Secretary of Defense, Information Management. *Business Process Reengineering. DOD Information Warfare Baseline Study Report*. Washington, DC: DOD, 5 June-21 July 1995. Provides a baseline activity model for current IW processes, identifies improvement opportunities and recommends a plan for the application of business process reengineering to IW; prepared by the DOD IW Team Working Group.

Downs, Lawrence G. *Digital Data Warfare: Using Malicious Computer Code as a Weapon*. Maxwell AFB, AL: US Air War College, Air University, April l995. Describes five phases of Digital Data Warfare (DDW)—penetration, propagation, dormancy, execution and termination; outlines an effective security program that would provide a defense against DDW.

Drake, William J., ed. *The New Information Infrastructure: Strategies for US Policy*. New York: The Twentieth Century Fund Press, 1995.

DSB. *Report of the Defense Science Board Summer Study Task Force on Information Architecture for the Battlefield. Final Report*. Washington, DC: DSB, October 1994. A 188-page report addressing four aspects of information architecture for the battlefield: use of information in warfare, use of I-AW, both offensive and defensive, the business practices of DOD in acquiring and using battlefield information systems and the underlying technology required to develop and implement these systems; expresses concern that DOD information systems are highly vulnerable to I-AW but that the information systems of potential adversaries are also quite vulnerable; concludes that management structure changes can provide an effective approach to integration of disparate systems and that DOD can greatly enhance the effectiveness of its limited resources by leveraging available commercial products and technology.

_____. *Report of the Defense Science Board Task Force on Defense Mapping for Future Operations. Final Report*. Washington, DC: DSB, September 1995. Concludes that DOD should provide a readily accessible source of digital information which will satisfy military geospatial, mapping, charting and weapon systems requirements and which should be accessible electronically to make a major contribution to battlefield information dominance and support the needs for modeling and simulation, wargaming, training, exercising, rehearsal, operations and poststrike analysis.

Emmett, P.C. "Software Warfare: The Emerging Future." *RUSI Journal*, December 1992, 56-60. Emphasizes the critical need for military theory to advance with the revolution in software technology.

Fitzsimonds, James R. "Coming Military Revolution: Opportunities and Risks." *Parameters*, Summer 1995, 30-36. Assesses military technology research developments.

Fogleman, Ronald R. "What Information Warfare Means

to You." *Air Force Times*, 17 July 1995, 31. Discusses the joint tactical information distribution system.

Francois, Kenneth et al. *Information Warfare on the Map: A Concept for Strategy-Making in the Information Age*. Washington, DC: School of Information Warfare and Strategy, NDU, 29 May 1996. Addresses the potential for mapping the virtual environment created by information technologies as a tool for developing I-AW strategies.

Gehly, Darryl. "Controlling the Battlefield." *Journal of Electronic Defense*, June 1993, 42-49. Examines the development and deployment of joint, interoperable C^4I architectures which will provide for the rapid exchange of information and analysis; discusses "C^4I for the Warrior" and Joint Tactical Information Distribution System, a "jam resistant, secure, high-capacity digital data and voice information distribution system."

Giboney, Thomas B. "Commander's Control From Information Chaos." *Military Review*, November 1991, 34-38. Describes the Commander's Critical Information Requirements methodology, an information management process designed to balance high technology and human resources.

Goodman, S.E. "War, Information Technologies and International Asymmetries." *Communications of the ACM*, December 1996, 11-16. Addresses US outspending of all other nations in the use of IT for military and intelligence purposes; discusses how some nations may address this asymmetry by acquiring nuclear or biological weapons or even some high technology to combat US military might.

Grange, David L. and James A. Kelley. "Victory through Information Dominance." *ARMY*, March 1997, 32-36. Discusses the US Army's IO.

Gray, Jim. "Turning Lessons Learned into Policy." *Journal of Electronic Defense*, October 1993, 87-92. Describes how the successes of EW in *Desert Storm* have led to significant changes; examines new capabilities and concepts to better integrate it into the joint commander's war plans.

Grier, Peter. "Preparing for 21st-Century Information War." *Government Executive*, August 1995, 130-32. Discusses predictions that defense electronics spending will amount to about $37 billion a year, with military aircraft the single biggest market category for defense electronics firms.

_____. "The Top Contract Categories: Electronics and Communications—Byting through the Fog of War." *Government Executive*, August 1994, 127-29. Reports on Army plans to spend a total of approximately $700 million on digital information technologies by 1999 for I-AW purposes.

Guenther, Otto and Robert F. Giordano. "Enabling Technologies and Advanced Concepts for the Digitized Force XXI." *Army RD&A Bulletin*, November-December 1994, 21-24.

Guibault, R.G. "Information Empowerment: The Key Force Multiplier." *Defense & Security Electronics*, January 1996, 10, 14.

Gunther, Judith et al. "Digital Warrior." *Popular Science*, September 1994, 60-64+. Describes 21st-century soldiers heavily armed with computers and nonlethal weapons.

Harknett, Richard J. "Information Warfare and Deterrence." *Parameters*, Autumn 1996, 93-107.

Harley, J.A *Information, Technology and the Center of Gravity*. Newport, RI: NWC, 14 June 1996; *National War College Review*, Winter 1997, 66-87. Discusses information and technology as tools with limitations that are not fully recognized.

Holzer, Robert. "Navy Eyes Single Command to Guide Info Warfare. *Navy Times*, 6 February 1995, 35. Reports on the establishment of the US Navy's Naval IW Activity as its focal point for I-AW activities.

Houghtaling, Pamela A. "New Information Warfare System Advances Army into Next Century." *Signal*, March 1996, 37-39. Deals with computers and tactical communications.

Hunt, Carl W. Commercial Systems Enhance Information Warfare Capability." *Signal*, March 1997, 64-65. Examines the asynchronous transfer mode telecommunications protocol and commercial-off-the-shelf (COTS) technologies which will improve DOD's ability to protect critical information and employ I-AW tools.

Hunter, Roger C. "Disabling Systems and the Air Force." *Airpower Journal*, Fall 1994, 43-47.

Hutcherson, Norman B. *Command and Control Warfare: Putting Another Tool in the War-Fighter's Data Base*. Research Report no. AU-ARI-94-1. Maxwell AFB, AL: Air University Press, September 1994. Discusses C^2W as the military strategy that implements IW, the objective of which is to attack the C^2 decision-making capabilities of an adversary while protecting friendly C^2 by disrupting and dominating the flow of information between the enemy's combat forces and their associated decision-making command elements.

"Information Warfare Center Stands up in Little Creek." *Marine Corps Gazette*, November 1995, 8-9. Reports on the formation and mission of the FIWC.

"Integration Efforts Mold Information Technology." *National Defense*, October 1994, 24+.

"IW Squadron to Evaluate Offensive Tactics." *Aviation Week & Space Technology*, 27 November 1995, 54. Reports on the 609th IW Squadron formed by the US Air Force to study personnel and operational requirements.

Johnson, Craig L. "Information Warfare—Not a Paper War." *Journal of Electronic Defense*, August 1994, 55-56+. Reports on the Air Force's IW center.

Johnson, Robert E. *Information Warfare: Impact on Command and Control Decision-Making*. Carlisle Barracks, PA: AWC, April 1996. Focuses on decision making when C^2 systems are interrupted, contaminated or destroyed and calls for contingency planning for disruptions in the flow of information.

Johnson, Stuart E. and Martin C. Libicki, ed. *Dominant Battlespace Awareness*. Washington, DC: Center for Advanced Concepts and Technology, Institute for National Strategic Studies, NDU Press, October 1995.

Joint Warfighting Science and Technology Plan. Washington, DC: Office of the Director of Defense Research and Engineering, May 96. A 215-page report concerning the technological advantage that has been a cornerstone of US national military strategy and the importance of maintaining a technological edge; discusses US warfighting capabilities 10 to 15 years in the future as substantially determined by current investment in science and technology.

Kahan, James P. et al. *Understanding Commander's Information Needs*. Santa Monica: RAND, 1989. Examines the interaction between command and information, centering on the commander's image or mental model of the battlefield and implications for education, training and information system design.

Kaminski, Paul G. "Sustaining Flight through Knowledge." *Defense Issues* 11/42 (1996), 1-4. Discusses military communications systems and I-AW issues.

Keuhl, Daniel. *Target Sets for Strategic Information Warfare in an Era of Comprehensive Situational Awareness*. School of Information Warfare and Strategy, NDU, 24 January 1995.

Killam, Timothy B. *Weapons of Mass Disruption For the Operational Info-Warrior*. Newport, RI: NWC, 12 February 1996. Defines I-AW as a way to control and attack the enemy's observation, orientation, decision and action loop.

Kincaid, William K. Jr. "Command, Control, Communications and Intelligence." *Aerospace America*, December 1992, 44-45. Reviews how computers and other high-technology equipment were integrated in the C^4I concept during 1992, giving rise to the C^4I program.

Kirk, David C. *Artificial Intelligence Applications to Information Warfare*. Carlisle Barracks, PA: AWC, 22 March 1996. Discusses artificial intelligence technology and intelligent agents that could help execute an information war by managing the information flow.

Lee, James G. *Counterspace Operations for Information Dominance*. Maxwell AFB, AL., School of Advanced Airpower Studies, Air University, October 1994. Assesses the effectiveness of current US space control strategy in an environment characterized by the increasing proliferation of space systems; offers an alternative space control strategy that focuses on attaining information dominance through the denial of information provided by space systems.

Leopold, George. "'Infowar': Can Bits Really Replace Bullets?" *Electronic Engineering Times*, 6 November 1995, 65-66. Discusses how the US can launch its own attacks in future wars and presents information on IW strategy.

Leugers, Jerry and Christopher Williams. "Satellite Comunications: Opening the Gateway to C^4I." *Surface Warfare*, July-August 1995, 16-17.

Libicki, Martin C. *The Mesh and the Net: Speculations on Armed Conflicts in a Time of Free Silicon*. Washington, DC: Center for Advanced Concepts and Technology, Institute for National Strategic Studies, NDU, March 1994. A 136-page study dealing with artificial intelligence, information transfer, man-computer interface, human-factors engineering and pop-up warfare.

_____. "Silicon and Security in the Twenty-First Century." *Strategic Review*, Summer 1992, 62-65.

Locke, Jeffrey S. *Command and Control Warfare: Promise and Challenge for the Operational Commander*. Newport, RI: NWC, 13 February 1995. Describes three areas of concern that need to be addressed if C^2W is to reach its full potential: the level of authority vested in the C^2W officer by the commander in chief or joint force commander, the need to focus on training and the need to define the relationship between I-AW and C^2W to ensure coordinated effort.

Loop, Tony. "Warfighter Information Network and the Next Generation of Switches." *Army Communicator: Voice of the Signal Corps*, Spring 1996, 8-14. Addresses military communications, computer networks, video imaging and recording technology and fiber-optic equipment and technology.

Lowrey, Dennis A. "Center without Walls: Training in the Information Age." *Military Intelligence*, October-December 1995, 45-48. Reports on training in the Army Intelligence Center at Fort Huachuca, Arizona.

Lum, Zachary A. "We Want the Airwaves: Defense on the C^2 (Command and Control) Front." *Journal of Electronic Defense*, June 1996, 37-40.

Macedonia, Michael R. "Information Technology in *Desert Storm*." *Military Review*, October 1992, 34-41. Focuses on how various computer and communications systems were used to plan, coordinate and disseminate the required information needed for the conduct of successful operations; discusses the relationship between command and decision making and IT and the need to develop appropriate doctrine, training and procedures.

"Marine Corps Information Warfare Combines Services' Needs, Defines Their Differences." *Signal*, July 1996, 61-62.

Mason, Jerry. "Operationalizing Information Warfare." *Surface Warfare*, September-October 1996, 33-35.

Matthews, William. "Girding for Cyberwar." *Air Force Times*, 18 July 1994, 36. Covers military IT, applications and technological and financial issues.

Matthys, Erick T. "Harnessing Technology for the Future." *Military Review*, May-June 1995, 71-76. Examines future information storage and retrieval systems.

Maxwell, Arthur G. Jr. *Joint Training for Information Managers*. Washington, DC: Center for Advanced Concepts and Technology, Institute for National Strategic Studies, NDU, May 1996.

Mayer, M.G. *Influence of Future Command, Control, Communications and Computers (C^4) on Doctrine and the Operational Commander's Decision-Making Process*. Newport, RI: NWC, 6 March 1996. Discusses C^4 systems which must manage and filter an overwhelming amount of information; covers interoperability issues, overcoming technological limitations, meeting emerging security requirements and protecting against I-AW; recommends unified control of C^4 systems under singular leadership for the common good of all the services and the revamping of acquisition policy and procedures to allow new technologies to be fielded quickly.

McAuliffe, Amy. "Building the Eyes and Ears of the Battlefield." *Military & Aerospace Electronics*, June 1995, 10-12. Covers the US military's use of sensor fusion and correlation in I-AW and the Army's All-Source Analysis System.

_____. "COTS Key to Info Warfare." *Military & Aerospace Electronics*, March 1995, 20. Discusses the DSB report titled "Information Architecture for the Battlefield" and the recommendation that DOD leverage commercial technology.

_____. "Information Warfare: Technology and Beyond." *Military & Aerospace Electronics*, December 1995, 6-8. Discusses offensive and defensive I-AW and lack of funds for simulation.

McAuliffe, Daniel J. "Command, Control, Communications and Intelligence." *Aerospace America*, December 1994, 35-36. Reviews recent advances in C^3I technology including vulnerabilities that may arise, attempts to enhance the flow of information to the field and other concerns associated with I-AW.

McKenzie, Kenneth F. Jr. "Beyond Luddites and Magicians: Examining the MTR." *Parameters*, Summer 1995, 15-21. Discusses military technology research (MTR) and development issues.

Mengxiong, Chang. *Prospects For Weapons, Troops and Battlefields In the Information Age*. Wright-Patterson AFB, OH: National Air Intelligence Center, 6 February 1996. Discusses weapons and troops in the 21st century as "informationized," such as informationized ammunition, informationized soldiers, informationized combat platform, defense information system (C^3I), informationized weapon system, informationized battlefield, I-AW and information intimidation; presents a methodology in studying weapons and troops of the 21st century.

Metz, Steven and James Kievit. "Siren Song of Technology and Conflict Short of War." *Special Warfare*, January 1996, 2-10.

Minihan, Kenneth. "Information Dominance: Meeting the Intelligence Needs of the 21st Century." *American Intelligence Journal*, March 1994, 15-19.

"Modern Battlefields Demand Stalwart Industry Practices." *Signal*, April 1996, 43-46.

Morrison, David C. "Bang! Bang! You've Been Inhibited!" *National Journal*, 28 March 1992, 758-59. Reports on nonlethal warfare, the creation of a new Nonlethal Warfare Study Group within the Pentagon and advantages and disadvantages of this type of warfare.

Morton, Oliver. "The Information Advantage." *The Economist*, 10 June 1995, 5-20. Focuses on the revolution in warfare technologies and the importance of information.

Munro, Neil. *The Quick and the Dead: Electronic Combat and Modern Warfare*. New York: St. Martin's Press, 1991.

Murphy, Dennis M. "Information Operations on the Nontraditional Battlefield." *Military Review*, November-December 1996, 16-18. Covers the role of I-AW in the US Army's concept of battlespace, the need to focus on the COG and think of battlespace as four-dimensional and options for the commander in viewing the enemy COG.

"Navy after Next: A Technology Vision of the Future." *Naval Research Reviews* 48/1 (1996), 32-37.

Naylor, Sean, D. "Info War." *Army Times*, 17 May 1993, 12-14. Examines the prospective improvements that digitization is expected to bring to the future battlefield.

Newell, Clayton R. "The Technological Future of War." *Military Review*, October 1989, 22-28. Covers the different impacts of technology on the strategic, operational and tactical levels of war and warns against technological change outpacing doctrine.

Newman, Richard J. "Ready! Aim! Reboot!" *U.S. News & World Report*, 20 January 1997, 45. Describes the use of IT in the US Army and its use in the expeditionary force exercise at Fort Hood, Texas.

Nichiporuk, Brian and Carl H. Builder. *Information Technologies and the Future of Land Warfare*. Santa Monica, CA: RAND Corporation, 1995.

Nifong, Michael R. "The Key to Information Dominance." *Military Review*, May-June 1996, 62-67.

Nowowiejski, Dean A. "Achieving Digital Destruction: Challenges for the M1A2 Task Force." *Armor*, January-February 1995, 21-24.

Owens, Admiral William A. "Emerging System of Systems." *US Naval Institute Proceedings*, May 1995, 35-39. Discusses C^4 issues, military planning and preparedness.

Paige, Emmett Jr. "Achieving the Integrated Systems Concept." *Defense Issues* 11/51 (1996), 1-4. Deals with standardization and interoperability aspects of information storage and retrieval systems.

Paylor, Mark A. *Command and Control (C^2) In Future Warfare*. Newport, RI: NWC, 6 March 1996. Concludes that although the "C^4I for the Warrior" technologies appear to effectively bridge the strategic and tactical levels of the military C^2 process structure, the operational commander performs vital operational-level functions in the C^2 process.

"Planners Seek New Models to Study Information Wars." *National Defense*, July-August 1996, 57. Outlines computer modeling and flight simulators.

Powell, Colin L. "Information-Age Warriors." *Byte*, July 1992, 370+. Reviews the use of computers in the Persian Gulf War, to include providing aircraft and missile target data, coordinating the flow of supplies and equipment into the area, maintaining personnel databases, planning routes, analyzing intelligence information, identifying the location of troops, moving messages across the battlefield and diagnosing radar systems; addresses problems of incompatibility and computer innovation outpacing interoperability.

Quinkert, Kathleen A. and Barbara A. Black. "Training for Force XXI Technologies." *Army RD&A Bulletin*, November-December 1994, 44-46.

Reese, W.D. *Command and Control in the Information Age*. Newport, RI: NWC, 14 June 1996. Stresses that senior commanders be cognizant of new commercial communications technology and its applicability in a myriad of military situations; describes recent advances in the commercial communications arena, especially fiber optic transmission systems and commercial communications satellites.

Reitlinger, Kurt C. "Command and Control for Third Wave Warfare." *ARMY*, February 1995, 9-14. Discusses C^2 systems for this type of warfare described by Alvin and Heidi Toffler as I-AW in which knowledge is the "central resource of destructivity."

Rhea, John. "The Dilemma of Using COTS in Electronic Warfare Systems." *Military & Aerospace Electronics*, September 1996, 8-10. Analyzes the dilemma over whether to replace traditional military-specific hardware with more affordable COTS equivalents wherever possible.

Richardson, Doug. "Confounding the Enemy: The Black Art of Infowar." *Defence '96: The World in Conflict* (1996), 155-59.

_____. "Information Warfare—New Threats and New Opportunities." *Asian Defence Journal*, April 1997, 50-55.

Rigby, Joe W. "Turning Point in Modernizing the Army . . . Acquiring the Digitized Force." *Army RD&A Bulletin*, November-December 1994, 16-17. Discusses military supplies, equipment and defense contract issues.

Robinson, Clarence A. Jr. "Army Information Operations Protect Command and Control." *Signal*, July 1996, 47-50.

_____. "Information Warfare Demands Battlespace Visualization Grasp." *Signal*, February 1997, 17-20. Addresses the challenge to help commanders understand information battlespace and IO, including decision process details and their execution in I-AW scenario.

Ross, Jimmy D. "Winning the Information War." *ARMY*, February 1994, 26-28+. Addresses C^3 issues.

Ryan, Donald E. Jr. "Implications of Information-Based Warfare." *JFQ*, Autumn-Winter 1994-1995, 114-16. Deals with military technology R&D.

Schneider, Michael W. *Electromagnetic Spectrum Domination: 21st Century Center of Gravity or Achilles Heel*. Fort Leavenworth, KS: SAMS, CGSC, 5 May 1994. A 65-page monograph dealing with the US Army's major peacetime modernization program which places a heavy premium on integrative technologies—computers and communications; discusses the increasing dependence on the electromagnetic spectrum to collect and move information on the 21st-century battlefield.

Scott, William B. "'Information Warfare' Demands New Approach." *Aviation Week & Space Technology*, 13 March 1995, 85-88. Reports on military leaders' acknowledgment that they must rely on private industry to provide technology, new security methods and efficient systems necessary to develop a cost-effective, space-based I-AW capability over the next decade.

_____. "New USAF Roadmaps Spotlight Space Warfare Technologies." *Aviation Week & Space Technology*, 6 January 1997, 59-61. Discusses the US Air Force's efforts to shift internal funds to systematically develop and field new space and I-AW technologies; reviews the findings of the Air Force Scientific Advisory Board's *New World Vistas* study.

Seagraves, Mary Ann and Richard J. Szymber. "Owning the Weather: The Environmental Side of the Information War." *Army RD&A Bulletin*, March-April 1995, 30-23.

Soo Hoo, Kevin J. *Strategic Information Warfare: A New Arena for Arms Control?* Stanford, CA: Center for International Security and Arms Control, Institute for International Studies, Stanford University, 1997.

Stewart, John F. Jr. "Command and Control Warfare and Intelligence on the Future Digital Battlefield." *Army RD&A Bulletin*, November-December 1994, 14-15.

Stewart, Michael J. *Information Operations, Information Warfare: Policy Perspectives and Implications for the Force*. Carlisle Barracks, PA: AWC, 1997. Discusses the effects of technological innovations on the armed forces.

Strassmann, Paul A. *Elements of an Information Management Doctrine for Low-Intensity Warfare*. Washington, DC: NDU, 20 January 1994. Asserts that sophisticated weapons with powerful destructive capacities will be of limited value in future low-intensity conflicts and that quick and precise deployment with superior C^{4}I capabilities is the key to successful operations; contends that information superiority is a prerequisite for military superiority.

Sullivan, Gordon R. "Force XXI: Digitizing the Battlefield." *Army RD&A Bulletin*, November-December 1994, 2-3. Deals with issues of military technology R&D and defense contracts and procurement.

Sweetnam, J.P. "New Thinking in the US Army: The Louisiana Manoeuvres, Battle Laboratories and the Third Wave Army." *Canadian Defence Quarterly*, September 1994, 23-28.

Szafranski, Richard. "Neocortical Warfare? The Acme of Skill." *Military Review*, November 1994, 41-55.

Tapscott, Mark. "New Pictures Emerging in Battlefield Intelligence." *Defense Electronics*, April 1993, 31-38. Surveys current technological advancements, such as digital imagery, data fusion and unmanned aerial vehicle surveillance, being made to better obtain and analyze battlefield intelligence; discusses DOD's effort to computerize C^{4}I functions in a drive for greater interoperability and effectiveness.

Tempestilli, Mark. "Network Force." *US Naval Institute Proceedings*, June 1996, 42-46.

_____. *Waging Information Warfare: Making the Connection Between Information and Power in a Transformed World*. Newport, RI: Joint Military Operations Department, NWC, 16 May 1995. Covers the emerging ways, means and ends of offensive I-AW in terms of target development, weaponeering, military options and organizing for action.

Thrasher, Roger D. *Information Warfare: Implications for Forging the Tools*. Monterey, CA: Naval Postgraduate School, June 1996. Analyzes the implications of dependence upon commercially available IT.

"The Ties that Bind." *Economist*, 10 June 1995, D18-20. Reports on encryption technology, weapons that disorient but do not kill, computer viruses and other innovations in technology.

Van Creveld, Martin. "High Technology and the Transformation of War: Part 1." *RUSI Journal*, October 1992, 76-81.

_____. "High Technology and the Transformation of War: Part 2." *RUSI Journal*, December 1992, 61-64.

Vandewart, R.L. and R.L. Craft. *Analytic Tools for Information Warfare*. Albuquerque, NM: Sandia National Laboratories 1996. Concerns I-AW and system surety—tradeoffs between system functionality, security, safety, reliability, cost and usability; describes one approach to surety assessment used at Sandia, identifies the difficulties in this process and proposes a set of features desirable in an automated environment to support this process.

Waller, Douglas and Mark Thompson. "Onward Cyber Soldiers." *Time*, 21 August 1995, 38-45. Examines various aspects of I-AW, to include technological achievements of the late 20th century which enable rapid and devastating attacks on the military and civilian infrastructure of an enemy, ethical problems created and how IW can enhance the management of an actual hot war.

Walsh, Robert S. "Information Enhancement on Today's Battlefield." *Marine Corps Gazette*, October 1995, 27-29. Discusses surveillance and technology issues.

Wardynski, E. Casey. "Labor Economics of Information Warfare." *Military Review*, May-June 1995, 56-61.

"Warfare in the Information Age: Cutting-edge Technology Helps Soldiers Keep the Peace in Bosnia." *Popular Science* 249/1 (1996), 52-57.

Washer, Thomas F. II. "Expanding the Division Communications Network on the Air-assault Battlefield." *Army Communicator: Voice of the Signal Corps*, Spring-Summer 1995, 15-18.

Williamson, John. "Winning the Data War." *Jane's Defence Weekly*, 20 May 1995, 44-46. Deals with tactical communications.

Wilson, G.I. and Frank Bunkers. "Uncorking the Information Genie." *Marine Corps Gazette*, October 1995, 29-31. Concerns military applications of computers and the information explosion.

Wood, J. Robert. "Lessons Learned in Information Age Warfare." *ARMY*, February 1996, 32-35. Discusses the 24th Infantry Division (Mechanized) Artillery's use of 21st-century hardware and software.

VII. Internet Sites

IW and Information Security on the Web from the Federation of American Scientists <http://www.fas.org/irp/wwwinfo.html>.

IW Resources from The Strategic Assessment Center, a division of Science Applications International Corporation <http://sac.saic.com/Iwlinks.htm>.

Institute for the Advanced Study of IW <http://www.psycom.net/iwar.1.html>.

Winn Schwartau's home page <http://www.infowar.com/>. ***MR***

NOTES

1. This project was completed under the auspices of a grant from the Institute for National Security Studies, US Air Force Academy, Colorado Springs, Colorado, during fiscal year 1997.

2. The author extends special thanks to the following individuals for their help in compiling this bibliography: Professor John Arquilla at the Naval Postgraduate School, who suggested the most useful subject categories to use and numerous pertinent sources for inclusion; Professor Thomas Czerwinski at the School of Information Warfare and Strategy, NDU, who provided me with a number of new publications of his and others at the school; and Navy Captain Richard O'Neil at the Pentagon's IO Directorate of the Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence, who provided additional hard-to-locate references for this project.

Timothy L. Sanz is research librarian, Research Library of the George C. Marshall European Center for Security Studies, Garmisch-Partenkirchen, Germany. He received a B.A. from Indiana University, an M.S.L.S. from the University of Kentucky and a Ph.D. from Ohio State University. He was previously a technical information specialist, Foreign Military Studies Office, Fort Leavenworth, Kansas, where he created and maintained an extensive database on foreign political-military affairs. He has published numerous bibliographies in European Security, Low-Intensity Conflict & Law Enforcement and Soviet Armed Forces Review Annual on various topics, including ethno-national conflicts, NATO's Partnership for Peace Program, the conflict in the former Republic of Yugoslavia, organized crime in the Russian Federation, peacekeeping and terrorism. His bibliography "Nuclear Terrorism: Published Literature Since 1992," appeared in the July-August 1997 edition of Military Review.